UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

SHERMAN MOORE on behalf of himself and all others similarly situated, Plaintiff, v. NETGAIN TECHNOLOGY, LLC, Defendant.	)	Case No. JURY TRIAL DEMANDED CLASS ACTION COMPLAINT

Plaintiff Sherman Moore ("Plaintiff"), by its undersigned counsel, files this Class Action Complaint on behalf of itself and a class of all similarly situated persons against Defendant Netgain Technology, LLC. ("Netgain" or "Defendant"). Plaintiff bases the forgoing allegations upon personal information and belief, the investigation of counsel, and state the following:

INTRODUCTION

1. Netgain is an external IT vendor that claims to provide "secure and scalable" information technology ("IT") and could-computing services for businesses. Specifically, Netgain specializes in serving the IT needs of two highly specialized and regulated industries: health care and accounting. Under Netgain's IT services model, its clients move their IT infrastructure into a cloud-based system that Netgain manages and oversees and uses to serve its clients' specific IT needs.

2. Due to specializing in healthcare and accounting, Netgain is responsible for managing and overseeing highly sensitive information. Its clients collect, store, and use

personal and confidential information that includes names, addresses, social security numbers, medical records and histories, and financial account information. As Netgain itself has acknowledged, this type of personal and sensitive data is highly targeted by hackers who seek to exploit that data for nefarious purposes. For example, fraudsters utilize medical information to secure medical procedures and bill the victim; attempt to utilize financial information to make fraudulent transactions and purchases; or use a collection of personal data to take out fraudulent loans. In the wrong hands, these types of sensitive and personal data may be wielded to cause significant harm to the patient's or individual's whose information is described in the records that Netgain, through its clients, stores.

3. Netgain assures its clients that it is a cybersecurity professional capable of keeping its clients' records (and the patients' and individuals' whose information is described in those records) safe. In fact, Netgain billed its services as offering "DoD-grade" and "ultra-secure protection" to its clients' data. Netgain also frequently published cybersecurity-related webinars that stressed the importance of maintaining adequate data security and offered advice on how to keep data safe and prevent a data breach.

4. In reality, Netgain's self-depiction as a cybersecurity expert proved false. Contrary to its many representations and promises, Netgain utilized inadequate data security measures it knew, or should have known, put the highly sensitive data it oversaw at significant risk of theft by or exposure to nefarious parties. Netgain, moreover, failed to meet the very cybersecurity standards that it had underscored as critical for its clients' businesses.

5. Consequently, from approximately September 2020 to December 2020, hackers breached Netgain's data environment and servers, accessed the highly sensitive data Netgain promised to secure, and stole copies of that data out of Netgain's servers ("Data Breach"). Later, Netgain would admit that it needed to implement a number of enhancements to its data security posture and deploy new tools to adequately protect its clients' data. Netgain acknowledged that it needed to make a "commitment" to keeping data security "top-of-mind"—a stark admission for a company that boasted of its "DoD-grade" cybersecurity and its specialized IT services for companies managing highly sensitive data.

6. The Data Breach impacted many of Netgain's clients, especially those in the healthcare industry, and those clients have already indicated that hundreds of thousands of records were impacted. The full scope of the Data Breach, however, is not known. In fact, Netgain appears to still be identifying which of its clients were affected by the Data Breach. On May 28, 2021, for instance, one of Netgain's former clients, Caravus, reported that data Netgain managed and stored more than 5 years ago had not been deleted securely and was included in the stolen data.

7. Plaintiff Sherman Moore's data was also included in the batch of information stolen during the Data Breach. Plaintiff received a notice from one of his medical providers notifying him that his data had been stolen. Around the same time, Plaintiff suffered from fraudulent transactions on one of his financial accounts and has also noticed an increase in spam directed towards him. Plaintiff remains at a continued risk of harm due to the exposure and potential misuse of his personal data by criminal hackers.

8. As such, Plaintiff brings this Complaint on behalf of persons whose personally identifying, health, financial, and other sensitive information was stolen during the Data Breach. Plaintiff asserts claims for negligence, negligence per se, and for declaratory and injunctive relief.

JURISDICTION

9. This Court has subject matter jurisdiction over this case pursuant to 28 U.S.C. § 1332(d), the Class Action Fairness Act, which affords federal courts with original jurisdiction over cases where any member of the plaintiff class is a citizen of a state different from any defendant, and where the amount in controversy exceeds $5,000,000, exclusive of interest and costs. Here, Plaintiff is diverse from Defendant because Plaintiff resides in Mississippi and Netgain resides in St. Cloud, Minnesota, where it is headquartered, and Delaware, where it is incorporated. Plaintiff alleges that, in the aggregate, the claims of all purported class members exceed $5,000,000, exclusive of interest and costs.

10. This Court has general personal jurisdiction over Netgain because Netgain is headquartered and operates its principal place of business in St. Cloud, Minnesota, including its principal and first ever data storage center. Netgain has minimum contacts with Minnesota because it is located there and conducts substantial business there.

11. This Court is the proper venue for this case pursuant to 28 U.S.C. § 1391(a) and (b) because a substantial part of the events and omissions giving rise to Plaintiff's claims occurred in Minnesota and because Minnesota conducts a substantial part of their business within this District.

PARTIES

12. **Plaintiff** Sherman Moore is a resident of Senatobia, Mississippi. Mr. Moore received a notice in the mail that his personal information may have been stolen during the Data Breach. After the Data Breach, Moore experienced a noticeable increase in spam email and suffered fraudulent transactions that required retaining separate legal counsel to resolve.

13. **Defendant** Netgain Technology, LLC is an external IT vendor providing ITaaS services, including IT-related and cloud-computing, to healthcare and accounting firms. Netgain is headquartered in St. Cloud, Minnesota, where it operates its headquarters and where it houses one of its principal data centers. Netgain is incorporated in Delaware.

BACKGROUND

A. Netgain Provides IT Services to Businesses with Highly Sensitive Data.

14. Netgain is a company located in St. Cloud, Minnesota that externally manages IT and cloud computing services on behalf of companies managing and overseeing highly sensitive data, including in healthcare and accounting industries.

15. Netgain describes its services as IT-as-a-service ("ITaaS"). Under Netgain's ITaaS business model, it moves its clients IT infrastructure "into a secure, cloud-based opex solution" that allows Netgain to tailor IT services specific to each clients' needs."[1] In other words, Netgain replaces traditional internal IT departments, and instead acts as an external IT vendor that, in addition to managing traditional IT needs, provides a host of

[1] *IT-as-a-Service (ITaaS)*, NetgainCloud.com (last visited, Jun. 10, 2020), https://netgaincloud.com/it-as-a-service/

other IT-related services, including, for example, cloud computing, technical infrastructure, IT management, and service and application management and security.

16. Netgain claims its ITaaS services offer a "better way" to deliver IT that allows it to "closely partner with accounting and healthcare clients to help navigate the industry's complex technological challenges and increasing regulations."[2] Netgain purports to offer "deep experience and specialization" and that its "IT and support professionals are fully committed to ensuring that [its clients] are pleased and [their] needs are fully met."[3]

17. Netgain also "pledge[s] to [its] clients that when they partner with Netgain, [its] team will deliver" and promises to, among other things: "Bring a business perspective and share exactly how the solutions will protect and support your business objectives and goals", "Remain on the leading edge of technology and stay current with the ever-changing needs and requirements of accounting and healthcare" and "Confirm your IT is running smoothly, and help to eliminate issues and loss of productivity."[4] It states that its "Vision" is to serve "customers in industries characterized by high compliance and high security" and that it provides its clients with "better technical knowledge, expertise, execution and confidence[.]"[5]

---

[2] *About Us*, NetgainCloud.com (last visited, Jun. 10, 2021), https://netgaincloud.com/about-us/

[3] *Id.*

[4] *Id.*

[5] *Id.*

18. Netgain's ITaaS services are specialized for businesses who manage highly sensitive data, specifically, businesses in the healthcare and accounting industries. Netgain, in fact, describes itself as a "leading outsourced provider of IT-as-a-Service" to customers in healthcare and accounting. Netgain, thus, must oversee, manage, and protect its clients' sensitive data that includes personally identifying information (like names, addresses, and social security numbers), healthcare information (like medical records and histories), and financial information (like payroll data and banking account information).

19. Given the highly sensitive nature of its clients' businesses, Netgain understood the need to protect that its clients' data and prioritize its data security. In fact, in 2017—long before Netgain's Data Breach—Netgain warned of the substantial costs of a data breach generally, and of a breach in the healthcare industry specifically.[6] It noted that a data breach cost healthcare companies approximately $380 per record exposed, and $141 per record in other industries.[7]

20. Netgain explained that, in particular, "[m]edical records are incredibly valuable to hackers because the data (names, addresses, social security numbers, medical history, insurance information, etc) is not easily changed."[8] As such, Netgain noted the healthcare industry annually spent over $6.2 billion on data breach-related costs.[9]

---

[6] *Understanding the True Cost of a Data Breach for Healthcare*, Netgain (Nov. 17, 2017), https://netgaincloud.com/blog/infographic-understanding-true-cost-data-breach-healthcare/.

[7] *Id.*

[8] *Id.*

[9] *Id.*

21. In the face of the risks of a data breach, Netgain advised that "Protecting your practice is crucial" and that "appropriate administrative and technical controls will mitigate your practice's vulnerability[.]"[10] Netgain provided examples of the types of controls that business should adopt, including: "Administrative Controls" like "conducting regular user training, hiring a dedicated security officer, employing and enforcing Bring Your Own Device (BYOD) policies and conducting extensive due diligence on third-party vendors" and "Technical Controls" like "patching and updating systems, automating your disaster recovery process and using anti-malware software."[11] Netgain also warned that compliance failures and failing to extensively use encryption would increase the costs of a data breach.[12]

22. Netgain portrayed itself as a data security expert to its clients and the public. It provided a host of cybersecurity-related webinars and presentations to its clients, including "Security Awareness Training", "Staying out of the Cybersecurity Headlines: Protecting Your Internal Cybersecurity Protects Your Organization," "Cybersecurity and Risk Management in 2020 – Planning and Protecting Your Firm" and "The Costs of Bad Security and How it Affects Your Organization."[13]

23. Netgain further represented that its company was fully capable of securing clients' highly sensitive medical and accounting data. It advertised that "The Netgain

---

[10] *Id.*

[11] *Id.*

[12] *Id.*

[13] *Cybersecurity Webinars*, NetgainCloud.com (last visited, Jun. 10, 2021), https://netgaincloud.com/webinar/cybersecurity-webinars/

Standard is included with every solution. Every time." The "Netgain Standard" including, among other things, "Cybersecurity", where Netgain promised to "Safeguard [clients'] sensitive data from tomorrow's threats with DoD-grade, ultra-secure protection."[14]

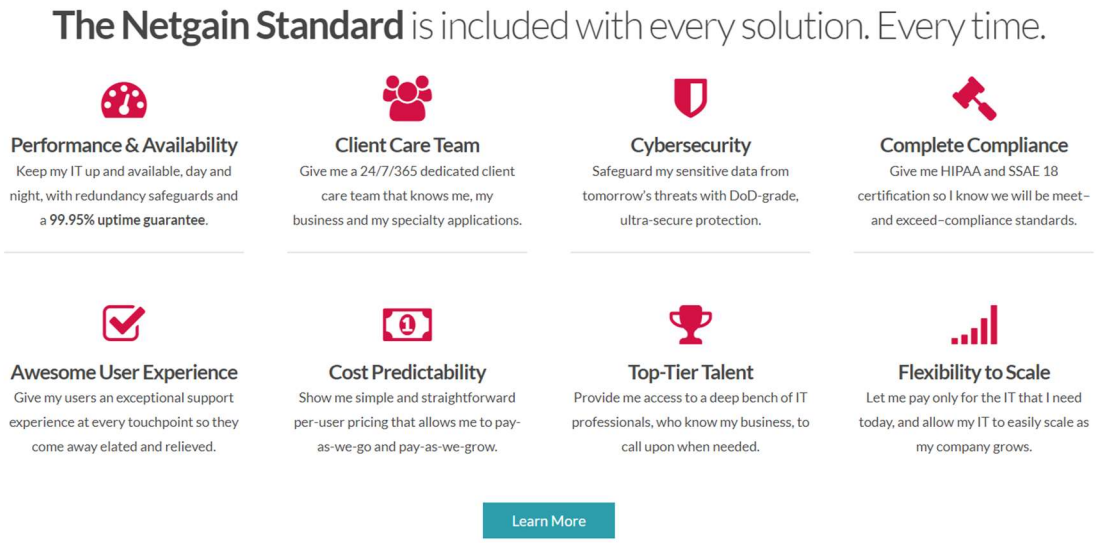

Image 1. Description of "The Netgain Standard."

24. Netgain also claimed it is "always there to keep your IT secure, available and performant."[15] Netgain's cybersecurity page states that: "Hackers don't sleep. But you can" and, further, that "Our security approach enables you to meet-and often exceed-compliance requirements while providing your staff with secure access to the information they need to do their jobs."[16]

[14] *The Netgain Standard*, NetgainCloud.com (last visited, Jun. 10, 2021), https://netgaincloud.com/why-netgain/.

[15] *See About Us*, *supra* note 2.

[16] *Cybersecurity at Netgain*, NetgainCloud.com (last visited, Jun. 10, 2021), https://netgaincloud.com/cybersecurity/

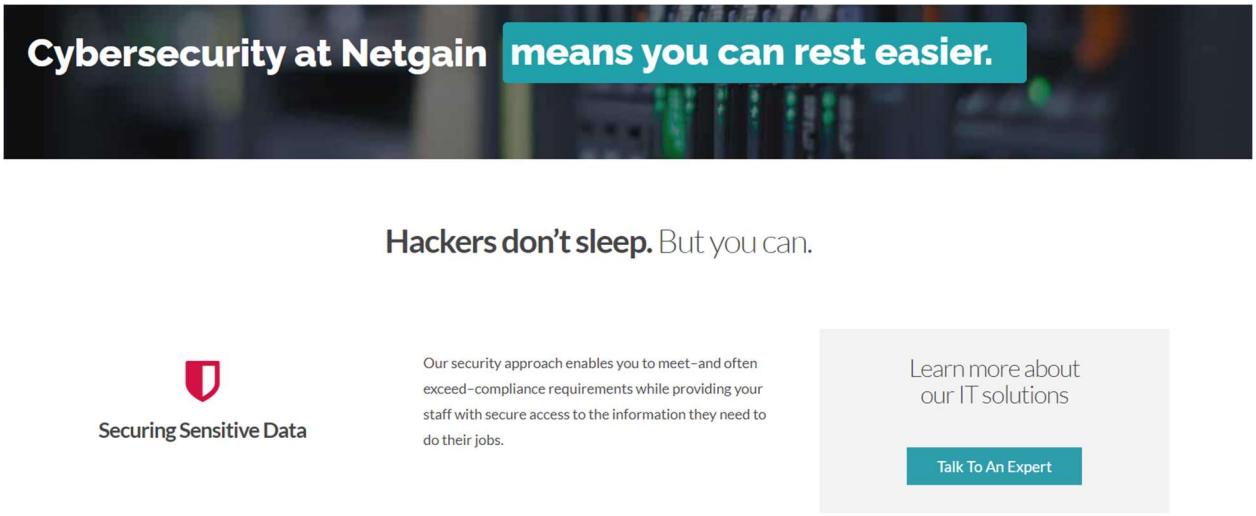

Image 2. A picture of Netgain's advertisement related to its cybersecurity services.

25. Finally, Netgain boasts that it houses "user data within the granite confines of a former Federal Building [to] ensure[] a level of structural stability that [its] clients [can] trust."[17]

26. Despite Netgain's promise protect client data and its effort to portray itself as a data security expert, Netgain's own data security decisions created substantial gaps that Netgain knew or should have known created a risk of a data breach. That risk materialized at the end of 2020, when hackers broke into Netgain's systems and stole highly sensitive data at will and put Plaintiff and the Class at risk that their data would be misused and cause them harm.

[17] *See About Us*, *supra* note 2.

B. Netgain Exposes Its Clients' Highly Sensitive Data to Hackers

27. From September to December 2020, hackers infiltrated Netgain and accessed, copied, and stole its clients' highly sensitive data.[18] Netgain did not report the data breach publicly, but rather, has sporadically issued notice to its clients starting in December 2020 and continuing to at least May 2021.

28. An article purporting to have obtained Netgain's notice to its clients reported that Netgain suffered a ransomware attack on November 24, 2020, requiring that Netgain take down "a number of [its] data centers . . . to contain this threat and restore services[.]"[19] The Data Breach involved an attack on Netgain's Domain Controllers that oversaw 1000s of servers, providing the hackers access to a substantial amount of highly sensitive data.

29. As a third-party IT service provider, Netgain had access to and controlled data from many, if not all, of its clients, and that data was stored on its servers. Netgain, thus, held a "master key" capable of "unlocking" each of its clients' "locks" put in place to protect the highly sensitive data stored on Netgain's servers. Had the hackers attacked Netgain's clients separately (assuming it was successfully), it might obtain that clients' specific data. By breaching Netgain, however, the hackers gained access to *all* (or a substantial portion of) Netgain's past and present clients' data that Netgain oversaw and managed.

---

[18] Lawrence Abrams, *Ransomeware forces hosting provider Netgain to take down data centers*, Bleeping Computer (Dec. 8, 2020), https://www.bleepingcomputer.com/news/security/ransomware-forces-hosting-provider-netgain-to-take-down-data-centers/.

[19] *Id.*

30. According to one of Netgain's clients, the hackers accessed portions of Netgain's data environment and successfully exfiltrated data out of Netgain's system.[20] In other words, the attack was a success and caused the theft of critical, sensitive data. The types of data confirmed or otherwise suspected to have impacted includes patient names, addresses, social security numbers, health information, medical records, bank records, financial account information, and drivers' license information.[21] This is the exact type of data Netgain had previously warned would be targeted by hackers and needed to be secured.

31. Despite the sensitive data impacted, Netgain has failed to provide full notice of the Data Breach and to identify which of its clients were affected. One provider, Woodcreek Provider Service ("Woodcreek"), who retained Netgain for its ITaaS services, disclosed "a security incident that involved unauthorized access to portions of the Netgain environment which Netgain had discovered in late November 2020 but may have occurred as early as September 2020."[22] Apparently, Woodcreek "received assurances that the attackers deleted the data and did not retain copies" and that Netgain paid the attackers a ransom. While, according to Woodcreek, Netgain's "experts continue to monitor for any

[20] *Woodcreek Provider Services Notifies More than 210,000 patients of Netgain Technology Ransome Incident*, DataBreaches.net (Mar. 5, 2021), https://www.databreaches.net/woodcreek-provider-services-notifies-more-than-210000-patients-of-netgain-ransomware-incident/

[21] *See, e.g.*, Lonut Llascu, *Netgain ransomware incident impacts local governments*, Bleeping Computer (Feb. 2, 2021), https://www.bleepingcomputer.com/news/security/netgain-ransomware-incident-impacts-local-governments/.

[22] *Woodcreek*, *supra* note 20.

signs that the data exfiltrated has been posted for sale[,]"[23] Netgain has not provided any public information about those efforts or the evidence they gathered regarding use and exfiltration of data.

32. Despite occurring in September to December of 2020, the scope of the Data Breach continues to be uncovered.[24] In fact, some of Netgain's clients are only just now learning that the Data Breach affected their data. In May 2021, nearly six months after the Data Breach, several companies—all current or former Netgain clients—learned for the first time that their data was impacted.[25] These include: Caravus, SouthCare Carolina, Jackson Thornton, San Diego Family Care, and Health Center Partners of Southern California.

33. On May 28, 2021, Caravus, an independent health care insurance broker in St. Louis, Missouri, issued a press release noting the "potential impact to some personal information as a result of a 2020 ransomeware attack on a former vendor, Netgain Technology, LLC[.]"[26] Carvus's investigation revealed that, despite having previously ending its contract with Netgain, Netgain's servers still retained Caravus's data from in or before 2016. As one security blogger put it: "for more than 5 years, [Caravus's] data sat

---

[23] *Id.*

[24] https://www.databreaches.net/it-seems-we-are-not-yet-done-hearing-about-the-netgain-technology-breach/

[25] *It seems we are not yet done hearing about the Netgain Technology Breach*, DataBreaches.net (May 11, 2021), https://www.databreaches.net/it-seems-we-are-not-yet-done-hearing-about-the-netgain-technology-breach/

[26] *Cavus impacted by Netgain Technology breach because vendor failed to destroy legacy data*, DataBreaches.net (May 28, 2021), https://www.databreaches.net/caravus-impacted-by-netgain-technology-breach-because-vendor-failure-to-destroy-legacy-data/.

on an old server and Netgain never securely deleted it or encrypted it at rest[.]"[27] The attackers ultimately compromised that unsecured and unnecessarily stored data.

34. In all, at this time, the known entities impacted by Netgain's Data Breach include: (1) Ramsey County, Minnesota, (2) Woodcreek Provider Services and MultiCare Health System, (3) Sandhill Medical Foundation, (4) Apply Valley Clinic/ Alina Health, (5) Neighborhood Healthcare, (6) San Diego Family Care, ad its associate, Health Center Partners of Southern California, (7) Jackson Thornton, (8) SouthCare Carolina, (9) Crystal Practice Management, and (10) SAC Health Systems.

35. Collectively, the impacted businesses have already reported hundreds of thousands of client and patient records impacted by the Data Breach. However, not all the impacted businesses have provided an indication of the number of records affected. Additionally, it is likely other, unknown or undisclosed entities were also affected.

36. What is clear, however, is that all the impacted companies provide healthcare or financial services, collect and maintain sensitive data, and trusted Netgain to do as it promised—to provide secure IT services that keep its data safe. Netgain failed to do so.

C. Netgain's Insufficient Data Security Caused the Data Breach

37. After the Data Breach, Netgain admitted that its data security was deficient and caused the Data Breach to occur. For instance, Netgain acknowledge that it "identified additional opportunities to strengthen [its] security posture" and needed to "implement[] a number of . . . identified enhancements to [its] security posture . . . to progress a multi-

[27] *Id.*

pronged [security] approach[.]"[28] These measures purportedly included "deploy[ing] new tools, revised policies and enforcement procedures, and implement[ing] an advanced around-the-clock managed detection and response service for proactive threat monitoring."[29] Netgain also acknowledged a need to make "an ongoing commitment to ensure [data security] remains top-of-mind."[30]

38. Furthermore, while Netgain boasts of the "new tools" it implemented to increase its security posture, those tools were not new to the data security industry. Rather, data security experts have been recommending those security measures be adopted for years beforehand.

39. For example, the "around the clock managed detection and response service" is part of the services provided by a Security Information and Event Monitoring System ("SIEM") designed to quickly identify indicators of an attack, issue warnings, and react to stop an intrusion early on. Data security experts have long recommended SIEM and other active monitoring systems in the healthcare industry to identify and respond to a data breach quickly and proactively.[31]

---

[28] Patrick Williamson, *What we learned as a ransomware victim – so you don't become one*, NetgainCloud.com (Mar. 24, 2021), https://netgaincloud.com/blog/what-we-learned-as-a-ransomware-victim-so-you-dont-become-one/

[29] *Id.*

[30] *Id.*

[31] Susan Biddle, *Why SIEM Solutions Are Essential to Securing Healthcare Networks*, Fortinet (Jun. 16, 2017), https://www.fortinet.com/blog/industry-trends/why-siem-solutions-are-essential-to-securing-healthcare-networks; Elizabeth O'Dowd, *Healthcare SIEM Provides Security Through Even Data Monitoring*, Hit Infrastructure (Dec. 31, 2017), https://hitinfrastructure.com/news/healthcare-siem-provides-security-through-event-data-monitoring.

40. Moreover, while Netgain now recognizes the need to make an "ongoing commitment" to data security and keep it "top-of-mind", security experts, including in the healthcare industry, have long warned companies that data security must be a top priority. The Department of Human Health and Services, in a series providing cybersecurity tips for those in the health care industry, wrote that:

> The tips in this document describe some ways to reduce the risk, decreasing the likelihood that patients' personal health information will be exposed to unauthorized disclosure, alteration, and destruction or denial of access. But none of these measures can be effective unless the health care practice is willing and able to implement them, to enforce policies that require these safeguards to be used, and to effectively and proactively train all users so that they are sensitized to the importance of information security. ***In short, each health care practice must instill and support a security-minded organizational culture***.[32]

41. The FTC has also issued numerous guidelines for businesses highlighting the importance of reasonable data security practices. The FTC notes the need to factor data security into all business decision-making.[33] According to the FTC, data security requires: (1) encrypting information stored on computer networks; (2) retaining payment card information only as long as necessary; (3) properly disposing of personal information that is no longer needed; (4) limiting administrative access to business systems; using industry tested and accepted security methods; (5) monitoring activity on networks to uncover

[32] *Top 10 Tips for Cybersecurity in Health Care*, Dept. of Health & Human Servs. (last visited, Jun. 10, 2021) (emphasis added), https://www.healthit.gov/sites/default/files/Top_10_Tips_for_Cybersecurity.pdf

[33] Federal Trade Comm'n, *Start with Security A Guide For Business, Lessons Learned from FTC Cases* (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

unapproved activity; (6) verifying that privacy and security features function properly; (7) testing for common vulnerabilities; and (8) updating and patching third-party software.[34]

42. The FTC treats the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5(a) of the FTC Act.

43. As such, the FTC has issued orders against businesses that failed to employ reasonable measures to secure sensitive payment card data. *See In the matter of Lookout Services, Inc.*, No. C-4326, ⁋ 7 (June 15, 2011) ("[Defendant] allowed users to bypass authentication procedures" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks, such as employing an intrusion detection system and monitoring system logs."); *In the matter of DSW, Inc.*, No. C-4157, ⁋ 7 (Mar. 7, 2006) ("[Defendant] failed to employ sufficient measures to detect unauthorized access."); *In the matter of The TJX Cos., Inc.*, No. C-4227 (Jul. 29, 2008) ("[R]espondent stored . . . personal information obtained to verify checks and process unreceipted returns in clear text on its in-store and corporate networks[,]" "did not require network administrators . . . to use different passwords to access different programs, computers, and networks[,]" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks . . ."); *In the matter of Dave & Buster's Inc.*, No. C-4291 (May 20, 2010) ("[Defendant] failed to monitor and filter outbound traffic from its

[34] *Id.*; Federal Trade Comm'n, *Protecting Personal Information, A Guide For Business* (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

networks to identify and block export of sensitive personal information without authorization" and "failed to use readily available security measures to limit access between instore networks . . ."). These orders, which all proceeded Netgain's Data Breach, further clarify the measures businesses must take to meet their data security obligations.

44. Although Netgain's business involves providing IT services related to the storage and maintenance of highly sensitive data, Netgain implemented inadequate data security practices that it knew or should have known, especially as a purported cybersecurity expert, put its clients and their customers at risk of having their sensitive data exposed.

45. After the Data Breach, however, Netgain attempted to downplay its role in causing the breach. Netgain began a series of blog posts billed as an effort to describe "what [Netgain] learned as a ransomware victim."[35] But, the blogposts read as an effort to divert blame.

46. In one post, Netgain claimed that "[n]o company or government agency is immune to cyberattacks" and noted other, apparently larger organizations, were also breached.[36] It also put the blame, in part, on the very clients' whose data Netgain exposed. Netgain wrote that:

> For too long, managed service providers and technology partners (including us) have taken the stance of shielding our clients from the headaches, intricacies, and complications that a strong security stance involves. While it's true that we can significantly reduce the burden of security on our clients and their teams, the responsibility is still shared. We owe it to our clients to

[35] Williamson, *supra* note 30.

[36] *Id.*

> ensure that they not only understand the steps we're taking as their IT partner, but also the measures that require their active participation and consent.[37]

47. In other words, despite Netgain's promise that it could and would protect its clients' highly sensitive data for them ("Hackers Don't Sleep. But you can.")—no doubt a critical factor in their decision to retain Netgain—after getting breached it claimed that *its clients* (who were not breached and who were not purportedly data security specialists) had a shared responsibility for the breach.

48. Netgain, thus, attempts to put the onus of data security onto its clients despite Netgain's supposed expertise in the matter and its representations that it would handle cybersecurity on their behalf. Perhaps the most salient advice Netgain provides is in its third blog post, where it directs clients to "[a]ddress security requirements with third parties, particularly if the organization outsourced the management and control of some of its information systems, networks and/or desktop environment." Netgain—being the very type of third party that controls its clients' IT systems—deserves to be scrutinized and heavily monitored by its clients because, as evidenced by the Data Breach, it cannot be trusted to protect highly sensitive data.

D. Netgain's Data Breach Harmed Plaintiff and the Class

49. As Netgain recognized, individual healthcare and financial records are specifically targeted by and extremely valuable to hackers.

50. Indeed, hackers increasingly sell these sensitive records on the black market to purchasers who seek to use the personally identifying information to create fake IDs,

[37] *Id.*

purchase medical equipment or drugs, file false insurance claims, make fraudulent transactions, or obtain loans.[38] One expert stated that for victims of medical record theft, "it's a 'mess.'"[39]

51. Hackers often use medical records containing personally identifying information to commit identity theft and fraudulent transactions. With medical and financial records, hackers can, among other things: purchase items online, extract money from victims' bank accounts, apply for bank loans and credit cards, make fraudulent health insurance claims, pay off their debt with the victim's money, or request money from a victim's contacts using social media and email.[40] Others suffer fraudulent financial transactions. It can be difficult to remove fraudulent procedures and transactions from a victim's medical and financial histories.

52. The risk of identity theft after a data breach is lasting. The U.S. Government Accountability Office's research into the effects of data breaches found that "in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data has been sold or posted on the Web, fraudulent use of that

[38] *What hackers actually do with your stolen medical records*, Advisory.com (Mar. 1, 2019), https://www.advisory.com/en/daily-briefing/2019/03/01/hackers

[39] *Id.*

[40] *How do hackers make money from your stolen data?*, Emsisoft.com (Feb. 20, 2020), https://blog.emsisoft.com/en/35541/how-do-hackers-make-money-from-your-stolen-data/

information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot rule out the significant risk of future harm."[41]

53. Plaintiff and the Class, thus, facing a continued risk that their sensitive data will be used for a nefarious purpose, causing them harm. Plaintiff already reported seeing a noticeable increase in phone and email spam, and recently had fraudulent transactions on his account that required the assistance of an attorney to address. Both the spam and fraudulent transactions occurred after the Data Breach, and therefore, were likely a direct result of the theft of Plaintiff's data from Netgain's servers. Plaintiff has not received any other notice of his data being compromised other than in Netgain's Data Breach.

CLASS ALLEGATIONS

54. Plaintiff brings this action on behalf of himself and all other similarly situated Class members pursuant to Rule 23(a), (b)(2) and (b)(3) of the Federal Rules of Civil Procedure and seek certification of the following Nationwide Class:

> All individuals that received or were otherwise sent notice that their data was potentially compromised due to Netgain's Data Breach.

55. Excluded from the class is Netgain and its subsidiaries and affiliates; all employees of Netgain; all persons who make a timely election to be excluded from the class; government entities; and the judge to whom this case is assigned and his/her immediate family and court staff.

[41] Report to Congressional Requesters, Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown 29 (Jun. 2007), http://www.gao.gov/new.items/d07737.pdf (last accessed Nov. 30, 2018).

56. Plaintiff reserves the right to, after conducting discovery, modify, expand or amend the above Class definition or to seek certification of a class or subclasses defined differently than above before any court determines whether certification is appropriate.

57. **Numerosity**. Consistent with Rule 23(a)(1), the members of the Class are so numerous and geographically dispersed that joinder of all Class members is impracticable. Plaintiff believes that there are hundreds of thousands of members of the Class. The number of reportedly impacted individuals already exceeds 100,000, and Plaintiff believes additional entities and persons may have been affected by the Data Breach. The precise number of class members, however, is unknown to Plaintiff. Class members may be identified through objective means. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

58. **Commonality and Predominance**. Consistent with Fed. R. Civ. P. 23(a)(2) and with 23(b)(3)'s commonality and predominance requirements, this action involves common questions of law and fact which predominate over any questions affecting individual Class members. These common questions include, without limitation:

a. Whether Netgain knew or should have known that its data environment and cybersecurity measures created a risk of a data breach;

b. Whether Netgain controlled and took responsibility for protecting Plaintiff's and the Class's data when it stored that data on its servers;

c. Whether Netgain's security measures were reasonable in light of the recommendations of the Department of Human Health and Services, the FTC data security recommendations, state laws and guidelines, and common recommendations made by data security experts;

d. Whether Netgain owed Plaintiff and the Class a duty to implement reasonable security measures;

e. Whether Netgain's failure to adequately secure Plaintiff's and the Class's data constitutes a breach of its duty to institute reasonable security measures;

f. Whether Netgain's failure to implement reasonable data security measures allowed the breach of its data systems to occur and caused the theft of Plaintiff's and the Class's data;

g. Whether reasonable security measures known and recommended by the data security community could have prevented the breach;

h. Whether Plaintiff and the Class were injured and suffered damages or other losses because of Netgain's failure to reasonably protect its data systems; and

i. Whether Plaintiff and the Class are entitled to relief.

59. **Typicality**. Consistent with Fed. R. Civ. P. 23(a)(3), Plaintiff is a typical member of the Class. Plaintiff and the Class are each persons whose medical or financial data resided on Netgain's servers because of contracts entered into between Netgain and healthcare and financial businesses that collected data from Plaintiff and the Class. Plaintiff's injuries are similar to other class members and Plaintiff seeks relief consistent with the relief due to the Class.

60. **Adequacy**. Consistent with Fed. R. Civ. P. 23(a)(4), Plaintiff is an adequate representative of the Class because Plaintiff is a member of the Class and is committed to pursuing this matter against Netgain to obtain relief for himself and for the Class. Plaintiff has no conflicts of interest with the Class. Plaintiff has also retained counsel competent and experienced in complex class action litigation of this type, having previously litigated

data breach cases. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

61. **Superiority**. Consistent with Fed. R. Civ. P 23(b)(3), class action litigation is superior to any other available means for the fair and efficient adjudication of this controversy. Individual litigation by each Class member would strain the court system because of the numerous members of the Class. Individual litigation creates the potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court. A class action would also permit financial institutions to recover even if their damages are small as compared to the burden and expense of litigation, a quintessential purpose of the class action mechanism.

62. **Injunctive and Declaratory Relief**. Consistent with Fed. R. Civ. P. 23(b)(2), Defendant, through its uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the class as a whole.

CLAIMS

COUNT I
Negligence

63. Plaintiff repeats and re-alleges the allegations contained in every preceding paragraph as if fully set forth herein.

64. Netgain owed a duty to Plaintiff and the members of the Class to take reasonable care in managing and protecting the highly sensitive data it managed and stored on behalf of its clients. This duty arises from multiple sources.

65. Netgain owed a common law duty to Plaintiff and the Class to implement reasonable data security measures because it was foreseeable that hackers would target Netgain's data systems and servers containing Plaintiff's and the Class's sensitive data and that, should a breach occur, Plaintiff and the Class would be harmed. Netgain alone controlled its technology, infrastructure, and cybersecurity. It further knew or should have known that if hackers breached its data systems, they would extract sensitive data and inflict injury upon Plaintiff and the Class. Furthermore, Netgain knew or should have known that if hackers accessed the sensitive data, the responsibility for remediating and mitigating the consequences of the breach would largely fall on individual persons whose data was impacted and stolen. Therefore, the Data Breach, and the harm it caused Plaintiff and the Class, was the foreseeable consequence of Netgain's unsecured, unreasonable data security measures.

66. Additionally, Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, required Netgain to take reasonable measures to protect Plaintiff's and the Class's sensitive data and is a further source of Netgain's duty to Plaintiff and the Class. Section 5 prohibits unfair practices in or affecting commerce, including, as interpreted and enforced by the FTC, the unfair act or practice by businesses like Netgain of failing to use reasonable measures to highly sensitive medical and financial data. Netgain, therefore, was required and obligated to take reasonable measures to protect data it possessed, held,

or otherwise used. The FTC publications and data security breach orders described herein further form the basis of Netgain's duty to adequately protect sensitive information. By failing to implement reasonable data security measures, Netgain acted in violation of § 5 of the FTCA.

67. Netgain is obligated to perform its business operations in accordance with industry standards. Industry standards are another source of duty and obligations requiring Netgain to exercise reasonable care with respect to Plaintiff and the Class by implementing reasonable data security measures that do not create a foreseeable risk of harm to Plaintiff and the Class.

68. Netgain breached its duty to Plaintiff and the Class by implementing unreasonable data security measures and by failing to keep data security "top-of-mind" despite understanding and, previously writing about, the risk of a data breach involving highly sensitive data like healthcare records. Netgain further admitted that, after the Data Breach, it "identified additional opportunities to strengthen [its] security posture" and needed to "implement[] a number of . . . identified enhancements . . . ."

69. Netgain was fully capable of preventing the Data Breach. Netgain, as a cybersecurity expert and IT professional, knew of data security measures required or recommended by the FTC, state laws and guidelines, and other data security experts which, if implemented, would have prevented the Data Breach from occurring at all, or limited and shortened the scope of the Data Breach. Netgain thus failed to take reasonable measures to secure its system, leaving it vulnerable to a breach.

70. As a direct and proximate result of Netgain's negligence, Plaintiff and the Class have suffered and will continue to suffer injury, including the ongoing risk that their data will be used nefariously against them or for fraudulent purposes.

COUNT II
Negligence *Per Se*

71. Plaintiff repeats and re-alleges the allegations contained in every preceding paragraph as if fully set forth herein.

72. Netgain's unreasonable data security measures and failure to timely notify Plaintiff and the Class of the Data Breach violates Section 5 of the FTC Act. Although the FTC Act does not create a private right of action, both require businesses to institute reasonable data security measures and breach notification procedures, which Netgain failed to do.

73. Section 5 of the FTCA, 15 U.S.C. §45, prohibits "unfair. . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by businesses like Netgain of failing to use reasonable measures to protect sensitive health and financial data. The FTC publications and orders described above also form the basis of Netgain's duty.[42]

74. Netgain violated Section 5 of the FTC Act by failing to use reasonable measures to protect sensitive health and financial data and by not complying with applicable industry standards. Netgain's conduct was particularly unreasonable given the

[42] *See supra*, note 75 (listing orders).

highly sensitive nature and amount of data it stored on its services and the foreseeable consequences of a Data Breach should Netgain fail to secure its systems.

75. Netgain's violation of Section 5 of the FTC Act constitutes negligence per se.

76. Plaintiff and the Class are within the class of persons Section 5 of the FTCA (and similar state statutes) was intended to protect. Additionally, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. The FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same type of harm suffered by Plaintiff and the Class.

77. As a direct and proximate result of Netgain's negligence per se, Plaintiff and the Class have suffered and continue to suffer injury.

COUNT III

Declaratory and Injunctive Relief

78. Plaintiff repeats and re-alleges the foregoing allegations as if fully set forth herein.

79. Under the Declaratory Judgment Act, 28 U.S.C. §§2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as those alleged herein, which are tortious and which violate the terms of the federal and state statutes described above.

80. An actual controversy has arisen in the wake of the Data Breach at issue regarding Defendant's common law and other duties to act reasonably with respect to safeguarding the data of Plaintiff and the Class. Plaintiff allege Netgain's actions in this respect were inadequate and unreasonable and, upon information and belief, remain inadequate and unreasonable. Additionally, Plaintiff and the Class continue to suffer injury due to the continued and ongoing threat of additional fraud against them or on their accounts.

81. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Netgain owed, and continues to owe a legal duty to secure the sensitive information with which it is entrusted, specifically including information pertaining to healthcare and financial records it obtains from its clients, and to notify impacted individuals of the Data Breach under the common law, Section 5 of the FTC Act;

b. Netgain breached, and continues to breach, its legal duty by failing to employ reasonable measures to secure its customers' personal and financial information; and

c. Netgain's breach of its legal duty continues to cause harm to Plaintiff and the Class.

82. The Court should also issue corresponding injunctive relief requiring Netgain to employ adequate security protocols consistent with industry standards to protect its clients' (*i.e.* Plaintiff's and the Class's) data.

83. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another breach of Netgain's data systems. If another breach of Netgain's data systems occurs, Plaintiff and the Class will not have an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages, while warranted to compensate Plaintiff and the Class for their out-of-pocket and other damages that are legally quantifiable and provable, do not cover the full extent of injuries suffered by Plaintiff and the Class, which include monetary damages that are not legally quantifiable or provable.

84. The hardship to Plaintiff and the Class if an injunction does not issue exceeds the hardship to Netgain if an injunction is issued.

85. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach, thus eliminating the injuries that would result to Plaintiff, the Class, and the public at large.

PRAYER FOR RELIEF

86. Wherefore, Plaintiff, on behalf of himself and the Class, requests that this Court award relief as follows:

a. An order certifying the class and designating Plaintiff as the Class Representative and their counsel as Class Counsel;

b. An award to Plaintiff and the proposed Class members of damages with pre-judgment and post-judgment interest;

c. A declaratory judgment in favor of Plaintiff and the Class;

d. Injunctive relief to Plaintiff and the Class;

e. An award of attorneys' fees and costs as allowed by law; and

f. An award such other and further relief as the Court may deem necessary or appropriate.

JURY TRIAL DEMANDED

87. Plaintiff hereby demands a jury trial for all the claims so triable.

Respectfully submitted,

Dated: June 17, 2021

/s/ Brian C. Gudmundson

Brian C. Gudmundson (MN Lic. #336695)
Michael J. Laird (MN Lic. #398436)
Rachel K. Tack (MN Lic. #399529)
ZIMMERMAN REED LLP
1100 IDS Center
80 South 8th Street
Minneapolis, MN 55402
Telephone: (612) 341-0400
Facsimile: (612) 341-0844
brian.gudmundson@zimmreed.com
michael.laird@zimmreed.com
rachel.tack@zimmreed.com